PCT/GB 2004 / 0 0 0 3 0 3

The Patent Office

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

REC'D 08 MAR 2004
WIPO PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 2 March 2004

THE PATENT OFFICE
24 JAN 2003
RECEIVED BY HAND

Patents Form 1/77

...nts Act 1977
...16)

The Patent Office

27JAN03 E779908-1 D01631
P01/7700 0.00-0301726.6

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form.)

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

Fee: £0

1. Your reference — LJH/P45632.GB01

2. Patent application number *(The Patent Office will fill in this part)* — 0301726.6 — 24 JAN 2003

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

ECEBS LIMITED
ECEBS HOUSE
68 DOBCROFT ROAD
MILLHOUSES
SHEFFIELD
SOUTH YORKSHIRE S7 2LS

Patents ADP number *(if you know it)* — 8275307001

If the applicant is a corporate body, give the country/state of incorporation — UNITED KINGDOM

4. Title of the invention — IMPROVED SMARTCARD

5. Full name, address and postcode in the United Kingdom to which all correspondence relating to this form and translation should be sent

Reddie & Grose
16 Theobalds Road
LONDON
WC1X 8PL

Patents ADP number *(if you know it)* — 91001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application *(If you know it)*	Date of filing *(day/month/year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day/month/year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*
   a) any applicant named in part 3 is not an inventor, or
   b) there is an inventor who is not named as an applicant, or
   c) any named applicant is a corporate body.
   See note (d))

   YES

Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document.

Continuation sheets of this form	
Description	3
Claim*(s)*	
Abstract	
Drawing*(s)*	2 +2

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature

Date
24 January 2003

12. Name and daytime telephone number of person to contact in the United Kingdom

L J HARLAND
020-7242 0901

Warning
After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

Patents Form 1/77

Once you have filled in the form you must remember to sign and date it.

For details of the fee and ways to pay please contact the Patent Office.

IMPROVED SMARTCARD

Smartcards are limited in memory size by the die size.

However, it has been appreciated that attaching a second memory chip such as a FLASH ROM can greatly extend the storage capacity. The problem with this, however, is that the security of the data must be as good as if it was stored internally to the smartcard device to be a useful.

An embodiment of a scheme for securing the data stored in an external memory (XMEM) attached to the Smartcard secure microcontroller will be described below, in detail, by way of example only, with reference to the drawings, in which:

Figure 1 illustrates the XMEM page structure;

This document details the low level design of the Smartcard operating system to Memory (XMEM) communication functions for securely communicating and storing data on an external Flash memory chip connected to a smartcard. These functions are called by higher-level function to read and update data in XMEM. The XMEM may be, for example, an ATMEL AT45DB321B 4Mbyte Serial Data Flash. Communication with the XMEM is done using the AT903232CS SPI hardware and one of the IO lines is used as the chip selected. However the principles would apply to any Smartcard micro-controller with available I/O to interconnect to a serial FLASH device.

Each XMEM page contains 528 bytes. The page structure is shown in Figure 1.The first 8 bytes (Page Header) contains a byte to indicate the page is not erased (value not 0xFF), 5 bytes of random data, 2 bytes indicating the page number and a 1 byte sequence member. The Page Header is followed by 512 bytes of data. The trailing 8 bytes contain the Page Header CBC encrypted with the 512 data bytes. The Page Header is not encrypted to allow the chip to derive the page keys.

Security and Reliability

The XMEM drivers provide implement the following features to enhance security and reliability.

- The 512 data bytes within a page are Triple DES CBC Encrypted. Any changes to the data will change and invalidate the MAC
- Each page contains an 8 byte 3DES MAC.
- Each page is cryptographically embedded with it page number to allow confirmation that the page read is the page requested. The page number is protected from modification by the page MAC.
- The Master DES keys used to derive the page keys are unique to the chip and generated automatically internally the first time the chip is reset. These DES keys cannot be read or updated externally.
- The DES keys to encrypt and sign a page are regenerated on each update to the page from the Master Key, random data, page number and page

sequence number. This is an additional security feature to increase the complexity of a known text attack to obtain the keys, as the keys and therefore the MAC change on each update of the page.

- Each Page contains a one byte sequence number that is incremented on each update to the page. The sequence numbers are verified on a page read operation. The sequence numbers do not start at a 0x00 but are initialised with a random number; therefore the sequence number cannot be derived from the number of total updates to the page. The use of page sequence numbers increases the complexity of the attack by supplying the same page with previous contents. Without a sequence number this would be possible, as the page would have a valid MAC and valid page number.
- All Updates to the XMEM are verified by reading the XMEM after programming.
- The HAL functions will attempt to read or update the page 3 times before exiting.
- If a page is found to be erased it is initialised to a random value on reading. It will not be possible then to erase a page externally to force a page of known erased value to be read internally.

Sequence Numbers

The ATMEL AT45DB321B (XMEM) contains 8192 pages FLASH memory. Each page of the XMEM has an individual sequence number (1 byte). A copy of the sequence number must be stored elsewhere to compare with the page when read. To stop the copy of the sequence number being modified it must be protected. This can be achieved by storing all of the sequence numbers internally to the smartcard. This may not be suitable, as it requires 8192 bytes of EEPROM to be reserved for the sequence numbers. This problem is solved by reserving 32 pages of XMEM to each store 256 sequence numbers of the other 8160 pages. These pages are protected as normal, but their sequence numbers are stores in the smartcard EEPROM.

High Level Overview

Figure 2 below details the call sequence for the External Read and Update page functions which are as follows.

ReadXMEMPage:

Void readXMEMPage(word pageNum)

This function will read a page from XMEM. The function will call the function getPageSeqNum to read the expected page sequence number to compare it with the page received.

The function will call the **doRead** function to perform the actual reading of the pages, decryption and MAC verification.

An error will be returned if the read page sequence number is incorrect.

updateXMEMPage:

void readXMEMPage(word pageNum)

This function will update a page in XMEM and requires the page to be previously read to retrieve the existing page sequence number.

This function will call the **loadPageKeys** functions to derive new keys for the page based on the page number, updated sequence number and random data.

This function will perform the actual updating of the XMEM page using the SPI hardware to send the program command and data to the XMEM chip.

This function will call the **doRead** function to verify the updated data programmed correctly in the XMEM.

doRead: (internal Function)

void doRead(word pageNum, byte mode)

This function will read a page from XMEM or verify a page in XMEM. It has two modes:

1. It will read the page, decrypt the data, calling the **loadPageKeys** to derive the page keys and check the MAC and page numbers are correct.

2. It will read the page to verify the encrypted data sent to update the XMEM page was programmed correctly.

loadPageKeys:

void loadPageKeys(byte mode, word pageNum)

This function will load the Keys to encrypt/decrypt a page and generates the key diversification string if updating a page using random data, the page number and the incremented page sequence number or when reading it uses the first XMEM page as the diversification string. The diversifications string is encrypted with the chip unique Master XMEM keys to give chip, page and sequence unique keys. The Keys are loaded into the DES hardware.

getPageSeqNum:

byte readXMEMPage(word pageNum)

This function will return the page sequence number for the page. This function may have is called by the readXMEMPage function to return the page sequence number. It will make a recursive call to the readXMEMPage function to read the XMEM page that contains the original page sequence number requested.

Figure 1

Page Header	Page Erase Indicator 1 byte	Random String 5 bytes	Page Number 2 bytes	Seq Num 1 byte
Page Data	512 bytes of data (CBC Encrypted_			
Page MAC	8 byte MAC (calculated over previous 520 bytes)			

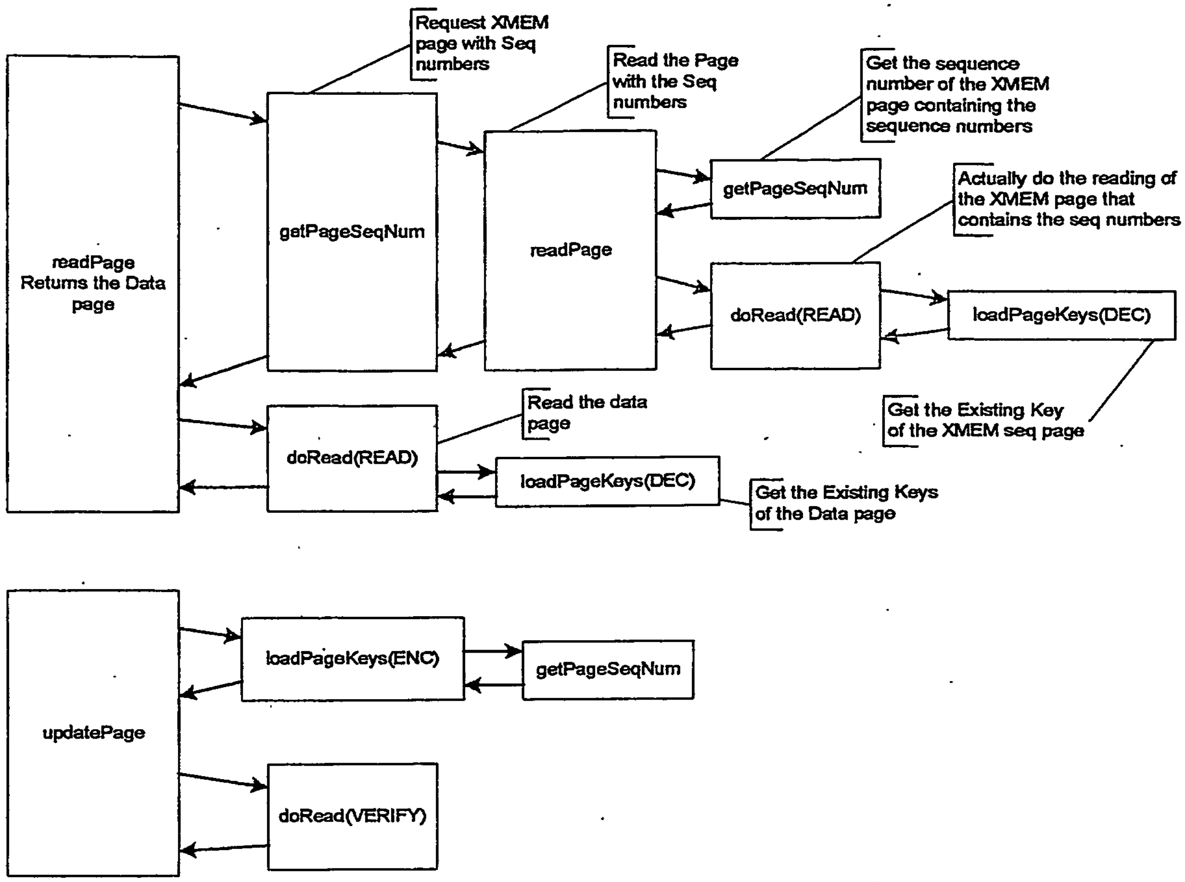
Request XMEM page with Seq numbers
Read the Page with the Seq numbers
Get the sequence number of the XMEM page containing the sequence numbers
readPage Returns the Data page
getPageSeqNum
readPage
getPageSeqNum
Actually do the reading of the XMEM page that contains the seq numbers
doRead(READ)
loadPageKeys(DEC)
Get the Existing Key of the XMEM seq page
Read the data page
doRead(READ)
loadPageKeys(DEC)
Get the Existing Keys of the Data page
updatePage
loadPageKeys(ENC)
getPageSeqNum
doRead(VERIFY)

Figure 2